(51) International Patent Classification⁷: H04L 9/00, G06F 15/16

(21) International Application Number:
PCT/US2004/036993

(22) International Filing Date:
8 November 2004 (08.11.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/517,868   7 November 2003 (07.11.2003)   US

(71) Applicant (for all designated States except US): CYOTA INC. [US/US]; 1350 Avenue of the Americas, New York, NY 10029 (US).

(72) Inventors; and
(75) Inventors/Applicants (for US only): GOLAN, Lior [IL/IL]; 3 Yehuda Halevi Street, 65135 Tel Aviv (IL). RIVNER, Nira [IL/IL]; 1a Smadar Street, Ramat Gan (IL). TSUR, Michal [IL/US]; 6724 Bonnie Ridge Dr 102, Baltimore, MD 21209 (US). ORAD, Amir; 43V Mizpe, P.O. Box 4718, Shoham 73142 (IL). BENNETT, Naftali [US/US]; 6 East 97 Street, New York, NY 10029 (US).

(74) Agent: POLLACK, Caleb; Eitan, Pearl, Latzer & Cohen Zedek, L.L.P., 10 Rockefeller Plaza, Suite 1001, New York, NY 10020 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LU, MC, NL, PL, PT, RO, SE,

(54) Title: SYSTEM AND METHOD OF ADDRESSING EMAIL AND ELECTRONIC COMMUNICATION FRAUD
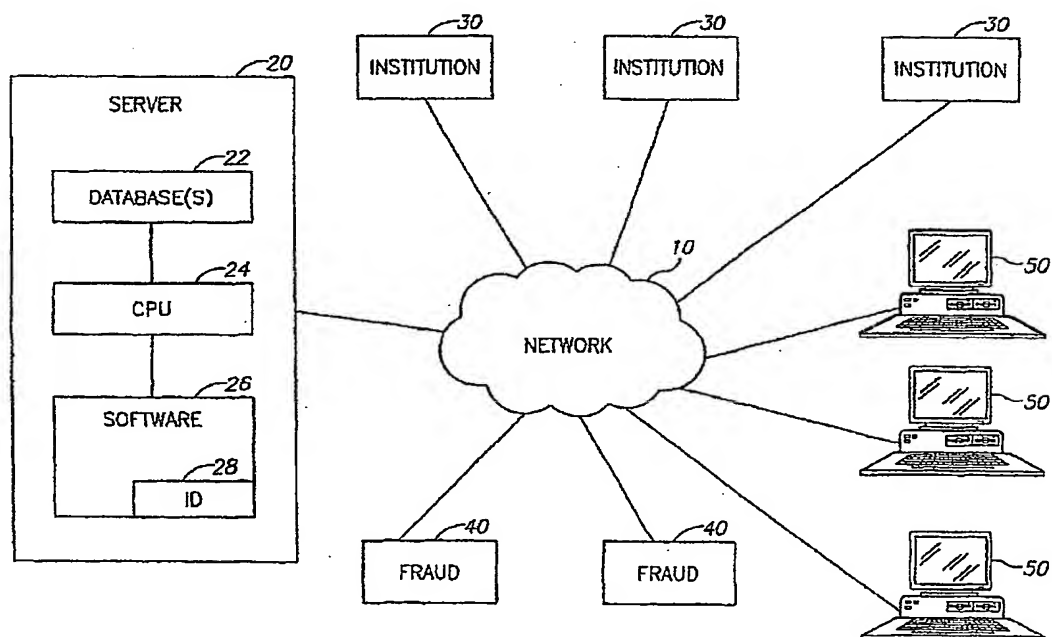
(57) Abstract: A system and method may respond to a fraudulent attack, such as a Phishing attack. The system and method may send a number of responses to party committing fraud, the responses designed to mimic the responses to' a Phishing attack. The responses may include codes or marked information designed to entrap or detect the party committing fraud.

SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.